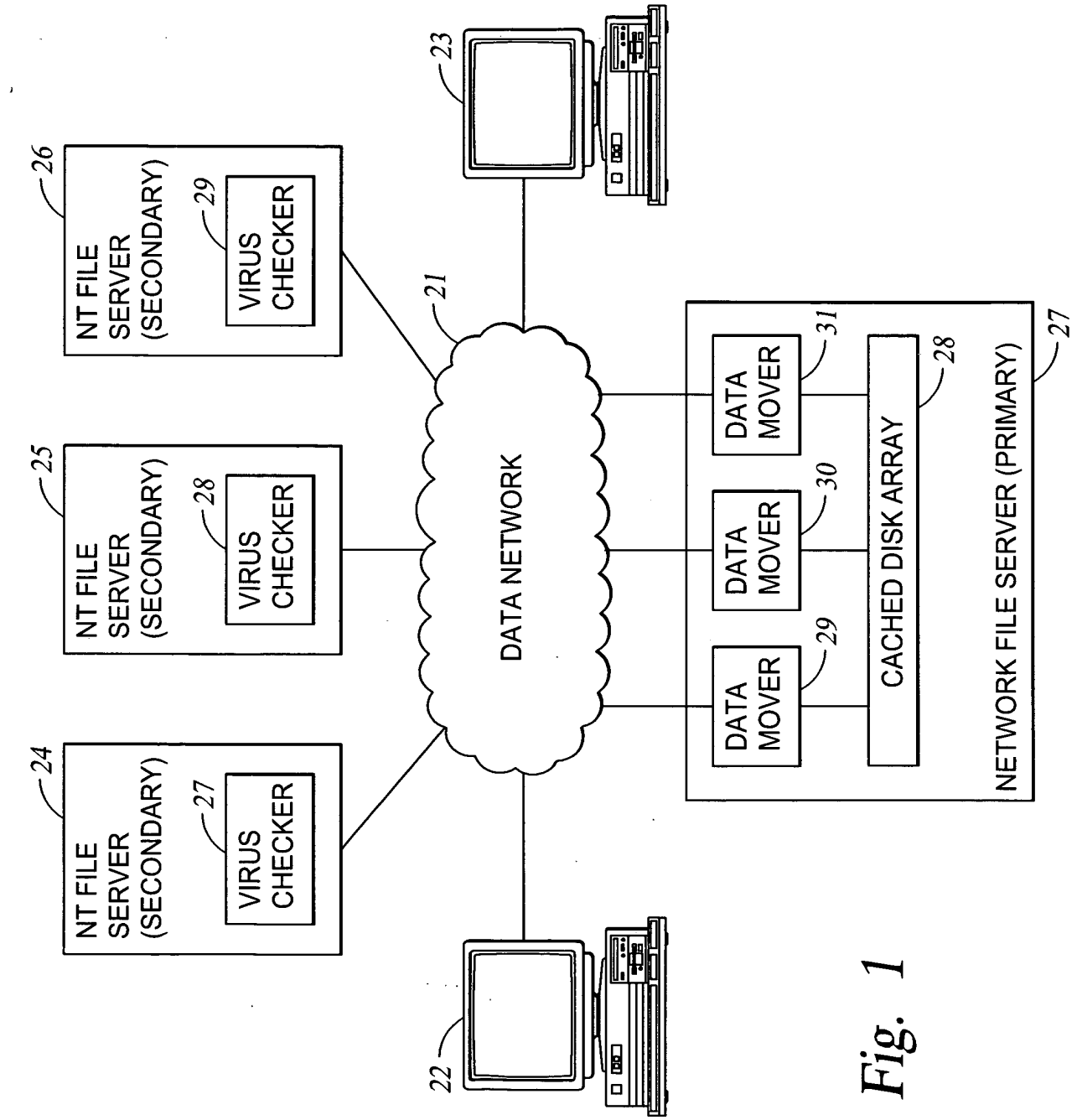
NT FILE SERVER (SECONDARY)
VIRUS CHECKER
26
29
NT FILE SERVER (SECONDARY)
VIRUS CHECKER
25
28
NT FILE SERVER (SECONDARY)
VIRUS CHECKER
24
27
23
21
DATA NETWORK
22
DATA MOVER
31
DATA MOVER
30
DATA MOVER
29
CACHED DISK ARRAY
28
NETWORK FILE SERVER (PRIMARY)
27

Fig. 1

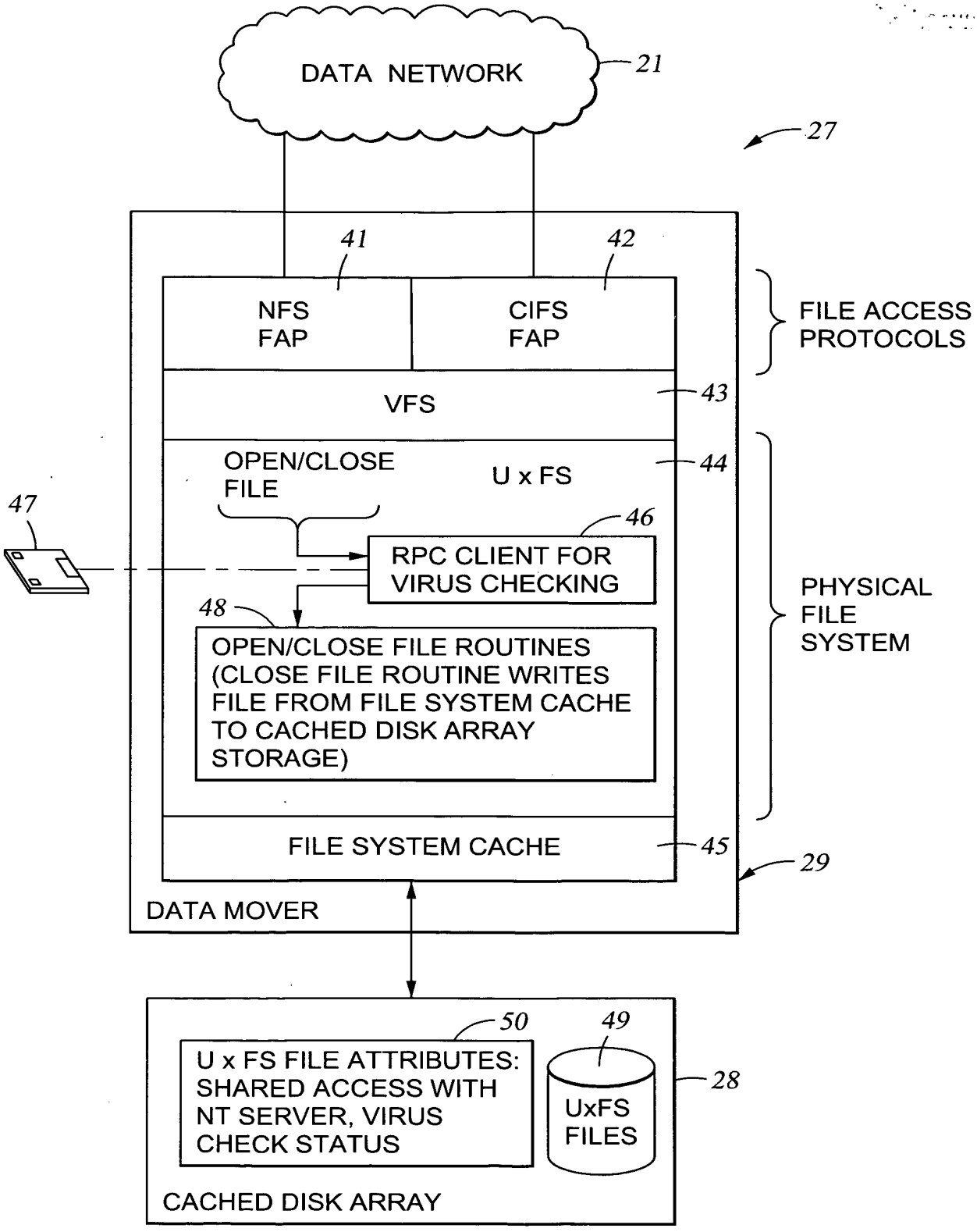
DATA NETWORK
21
27
41
42
NFS FAP
CIFS FAP
FILE ACCESS PROTOCOLS
VFS
43
OPEN/CLOSE FILE
U x FS
44
47
46
RPC CLIENT FOR VIRUS CHECKING
48
OPEN/CLOSE FILE ROUTINES (CLOSE FILE ROUTINE WRITES FILE FROM FILE SYSTEM CACHE TO CACHED DISK ARRAY STORAGE)
PHYSICAL FILE SYSTEM
FILE SYSTEM CACHE
45
29
DATA MOVER
50
49
U x FS FILE ATTRIBUTES: SHARED ACCESS WITH NT SERVER, VIRUS CHECK STATUS
UxFS FILES
28
CACHED DISK ARRAY

Fig. 2

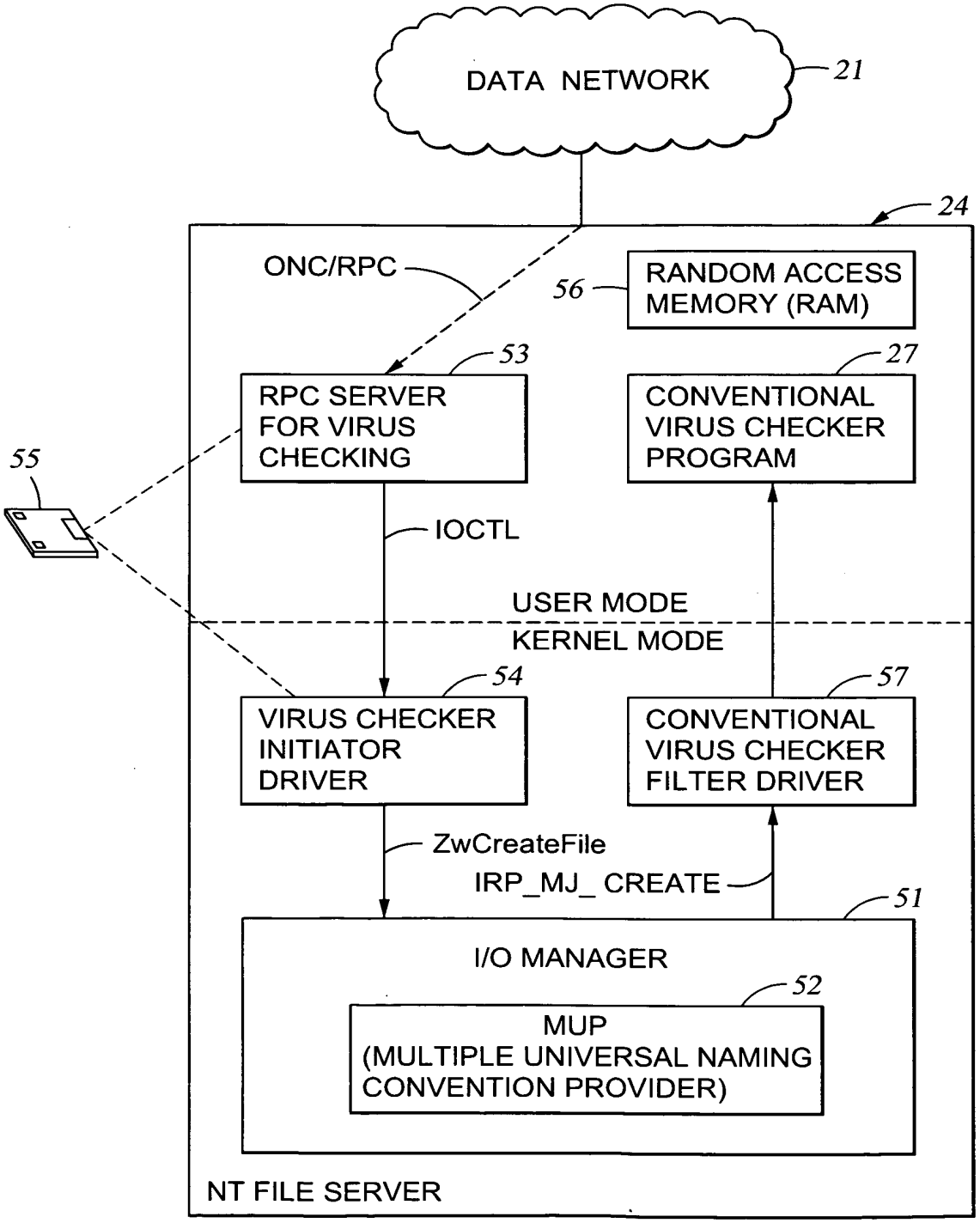
DATA NETWORK
21
24
ONC/RPC
56
RANDOM ACCESS MEMORY (RAM)
53
27
RPC SERVER FOR VIRUS CHECKING
CONVENTIONAL VIRUS CHECKER PROGRAM
55
IOCTL
USER MODE
KERNEL MODE
54
57
VIRUS CHECKER INITIATOR DRIVER
CONVENTIONAL VIRUS CHECKER FILTER DRIVER
ZwCreateFile
IRP_MJ_ CREATE
51
I/O MANAGER
52
MUP
(MULTIPLE UNIVERSAL NAMING CONVENTION PROVIDER)
NT FILE SERVER

Fig. 3

65

FILE ATTRIBUTES FOR VIRUS CHECKING		
BIT 0	BIT 1	STATUS
0	0	NOT CHECKED
0	1	CHECKING
1	0	CHECKED - OK
1	1	INFECTED

Fig. 4

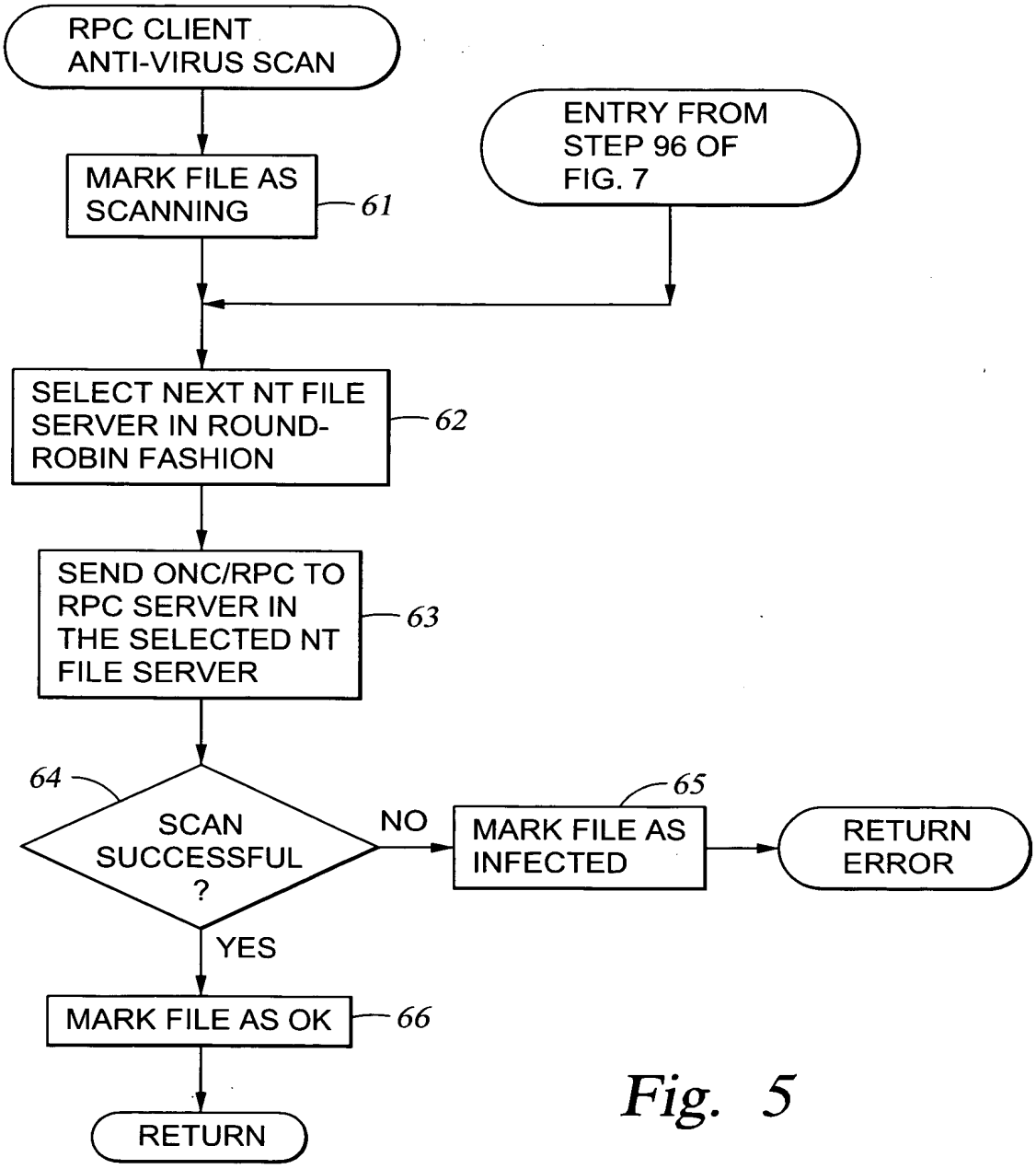
RPC CLIENT ANTI-VIRUS SCAN
ENTRY FROM STEP 96 OF FIG. 7
MARK FILE AS SCANNING
61
SELECT NEXT NT FILE SERVER IN ROUND-ROBIN FASHION
62
SEND ONC/RPC TO RPC SERVER IN THE SELECTED NT FILE SERVER
63
64
SCAN SUCCESSFUL ?
NO
65
MARK FILE AS INFECTED
RETURN ERROR
YES
MARK FILE AS OK
66
RETURN

Fig. 5

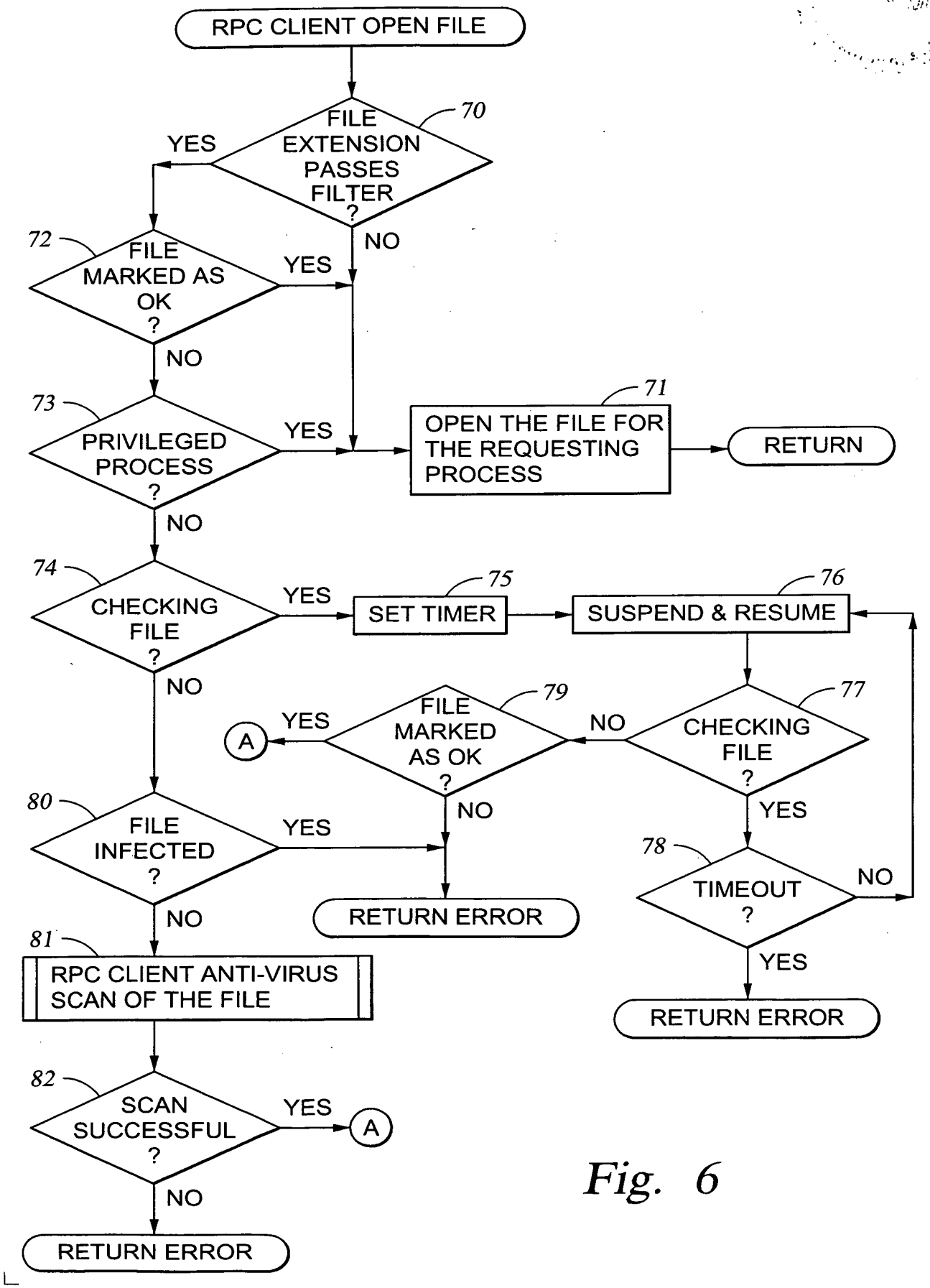
RPC CLIENT OPEN FILE
70
FILE EXTENSION PASSES FILTER ?
YES
NO
72
FILE MARKED AS OK ?
YES
NO
73
PRIVILEGED PROCESS ?
YES
NO
71
OPEN THE FILE FOR THE REQUESTING PROCESS
RETURN
74
CHECKING FILE ?
YES
NO
75
SET TIMER
76
SUSPEND & RESUME
79
FILE MARKED AS OK ?
YES
A
NO
77
CHECKING FILE ?
NO
YES
80
FILE INFECTED ?
YES
NO
RETURN ERROR
78
TIMEOUT ?
NO
YES
RETURN ERROR
81
RPC CLIENT ANTI-VIRUS SCAN OF THE FILE
82
SCAN SUCCESSFUL ?
YES
A
NO
RETURN ERROR

Fig. 6

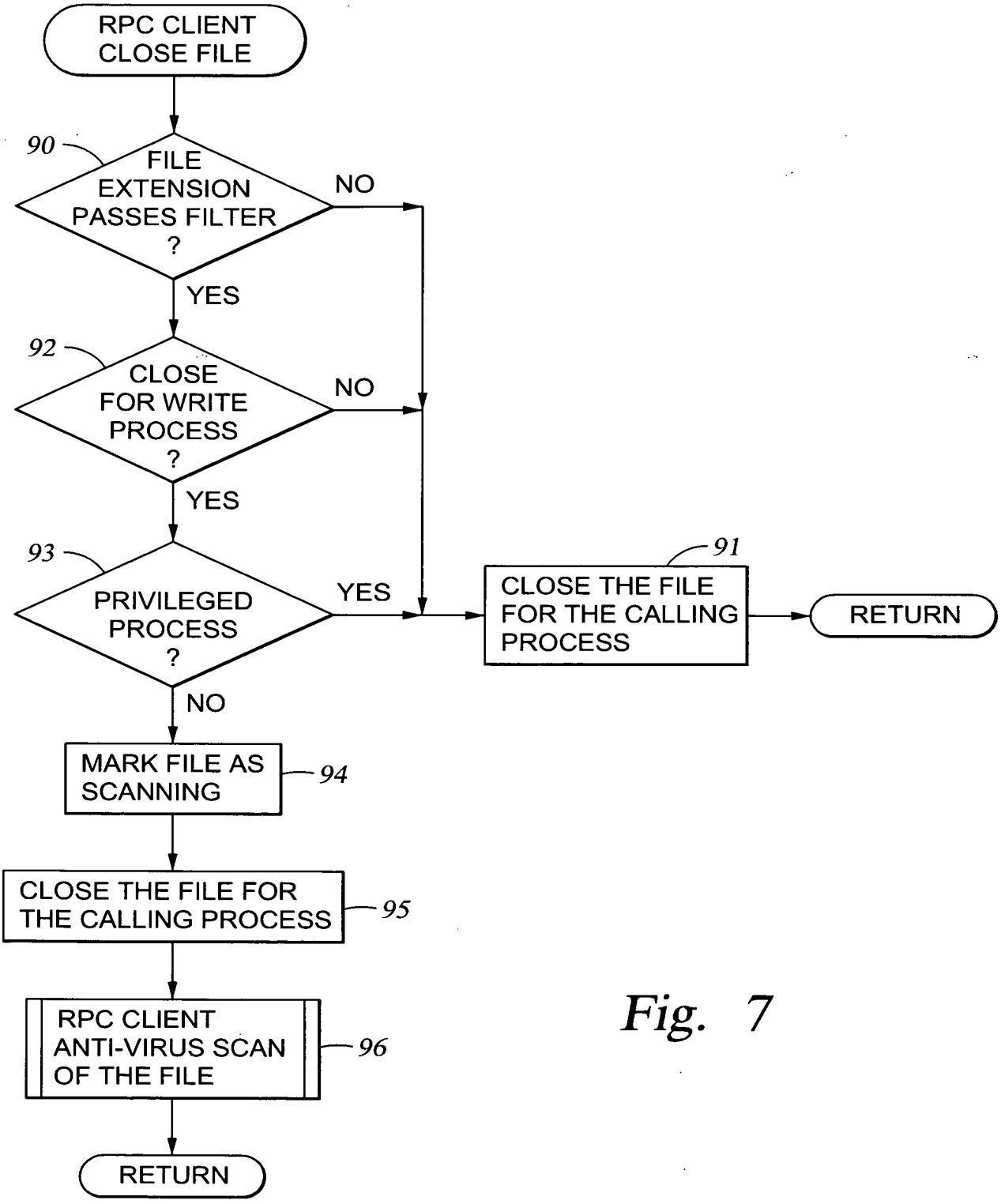
RPC CLIENT CLOSE FILE
90
FILE EXTENSION PASSES FILTER ?
NO
YES
92
CLOSE FOR WRITE PROCESS ?
NO
YES
93
PRIVILEGED PROCESS ?
YES
91
CLOSE THE FILE FOR THE CALLING PROCESS
RETURN
NO
MARK FILE AS SCANNING
94
CLOSE THE FILE FOR THE CALLING PROCESS
95
RPC CLIENT ANTI-VIRUS SCAN OF THE FILE
96
RETURN

Fig. 7

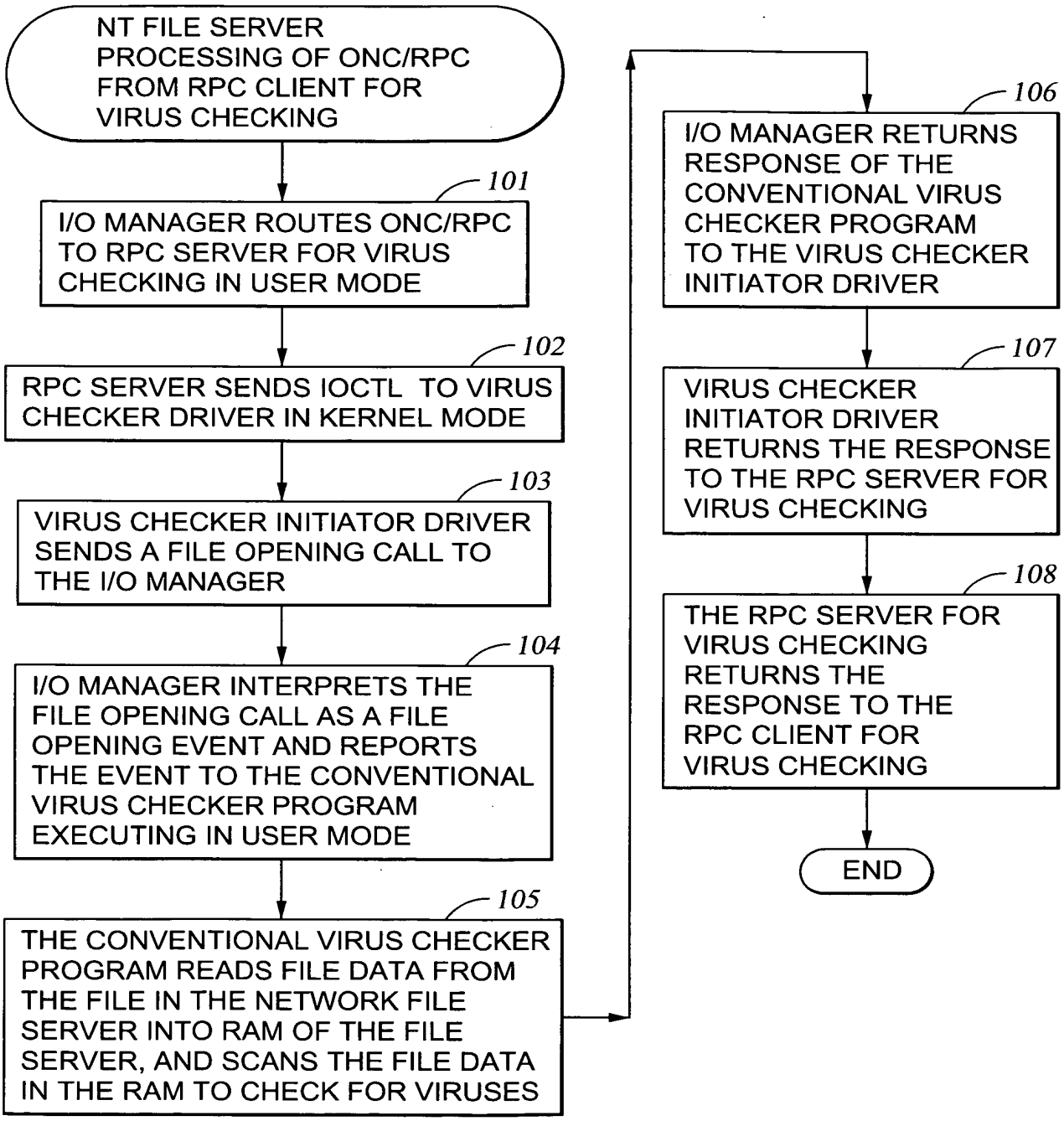
NT FILE SERVER PROCESSING OF ONC/RPC FROM RPC CLIENT FOR VIRUS CHECKING
101
I/O MANAGER ROUTES ONC/RPC TO RPC SERVER FOR VIRUS CHECKING IN USER MODE
102
RPC SERVER SENDS IOCTL TO VIRUS CHECKER DRIVER IN KERNEL MODE
103
VIRUS CHECKER INITIATOR DRIVER SENDS A FILE OPENING CALL TO THE I/O MANAGER
104
I/O MANAGER INTERPRETS THE FILE OPENING CALL AS A FILE OPENING EVENT AND REPORTS THE EVENT TO THE CONVENTIONAL VIRUS CHECKER PROGRAM EXECUTING IN USER MODE
105
THE CONVENTIONAL VIRUS CHECKER PROGRAM READS FILE DATA FROM THE FILE IN THE NETWORK FILE SERVER INTO RAM OF THE FILE SERVER, AND SCANS THE FILE DATA IN THE RAM TO CHECK FOR VIRUSES
106
I/O MANAGER RETURNS RESPONSE OF THE CONVENTIONAL VIRUS CHECKER PROGRAM TO THE VIRUS CHECKER INITIATOR DRIVER
107
VIRUS CHECKER INITIATOR DRIVER RETURNS THE RESPONSE TO THE RPC SERVER FOR VIRUS CHECKING
108
THE RPC SERVER FOR VIRUS CHECKING RETURNS THE RESPONSE TO THE RPC CLIENT FOR VIRUS CHECKING
END

Fig. 8

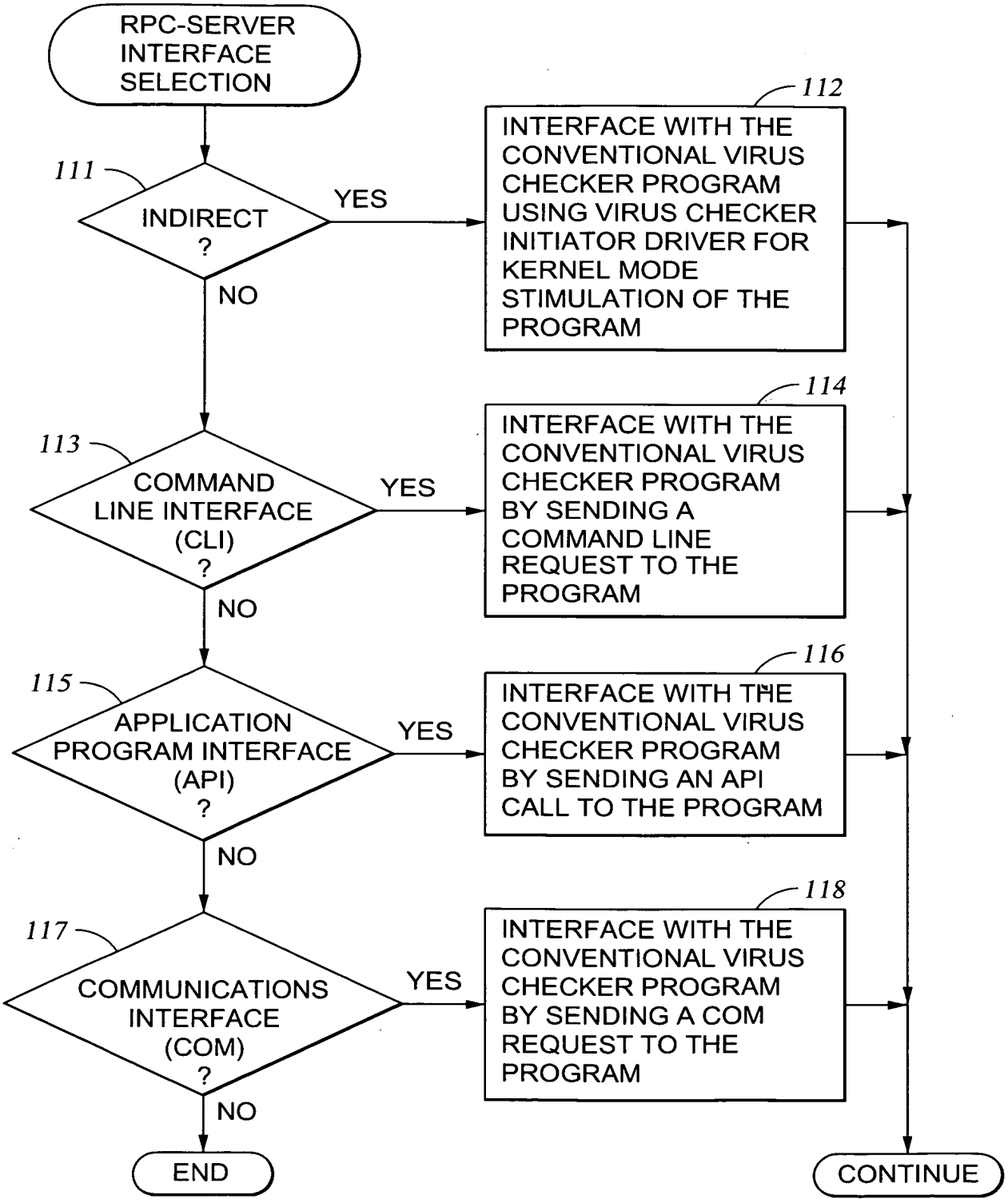
RPC-SERVER INTERFACE SELECTION
111
INDIRECT ?
YES
NO
112
INTERFACE WITH THE CONVENTIONAL VIRUS CHECKER PROGRAM USING VIRUS CHECKER INITIATOR DRIVER FOR KERNEL MODE STIMULATION OF THE PROGRAM
113
COMMAND LINE INTERFACE (CLI) ?
YES
NO
114
INTERFACE WITH THE CONVENTIONAL VIRUS CHECKER PROGRAM BY SENDING A COMMAND LINE REQUEST TO THE PROGRAM
115
APPLICATION PROGRAM INTERFACE (API) ?
YES
NO
116
INTERFACE WITH THE CONVENTIONAL VIRUS CHECKER PROGRAM BY SENDING AN API CALL TO THE PROGRAM
117
COMMUNICATIONS INTERFACE (COM) ?
YES
NO
118
INTERFACE WITH THE CONVENTIONAL VIRUS CHECKER PROGRAM BY SENDING A COM REQUEST TO THE PROGRAM
END
CONTINUE

Fig. 9

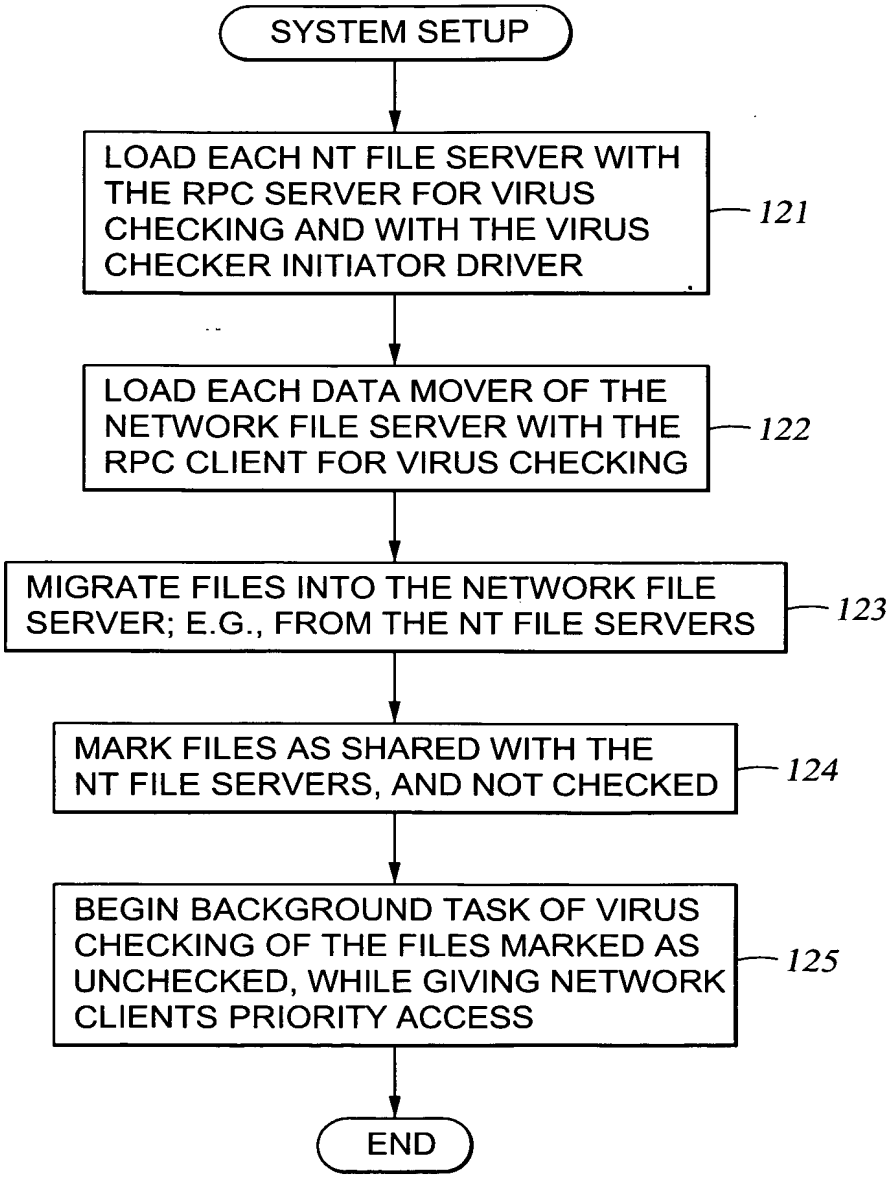
SYSTEM SETUP
LOAD EACH NT FILE SERVER WITH THE RPC SERVER FOR VIRUS CHECKING AND WITH THE VIRUS CHECKER INITIATOR DRIVER
121
LOAD EACH DATA MOVER OF THE NETWORK FILE SERVER WITH THE RPC CLIENT FOR VIRUS CHECKING
122
MIGRATE FILES INTO THE NETWORK FILE SERVER; E.G., FROM THE NT FILE SERVERS
123
MARK FILES AS SHARED WITH THE NT FILE SERVERS, AND NOT CHECKED
124
BEGIN BACKGROUND TASK OF VIRUS CHECKING OF THE FILES MARKED AS UNCHECKED, WHILE GIVING NETWORK CLIENTS PRIORITY ACCESS
125
END

Fig. 10